Trusler, kommunikation, nytte

Udfordringer ved offentlig-privat samarbejde om IKT-sikkerhed

Christensen, Kristoffer Kjærgaard; Lacoppidan, Oscar Vejen; Petersen, Karen Lund

Publication date:
2015

INSTITUT FOR STATSKUNDSKAB
KØBENHAVNS UNIVERSITET

Trusler, kommunikation, nytte:

Udfordringer ved offentlig-privat samarbejde om IKT-sikkerhed

Kristoffer Kjærgaard Christensen, Oscar Vejen Lacoppidan og Karen Lund Petersen
CAST og NordSTEVA

Resume

I dette policy brief peger vi på tre overordnede udfordringer ved at etablere offentlig-privat samarbejde om IKT-relaterede sikkerhedsspørgsmål. For det første opererer de forskellige aktører med **uens trusselsforståelser og –billeder**, hvilket bl.a. kommer til udtryk i den måde, man organiserer og orienterer sig på. Divergensen ses såvel i myndighedernes og virksomhedernes respektive tilgange til disse sikkerhedsspørgsmål som i ansvarsfordelingen myndighederne imellem. For det andet peger policy briefet på, at kommunikationen mellem myndigheder og virksomheder er en væsentlig udfordring. På dette område **efterspørger alle partner et tydeligere fokus samt mere dialog og vidensdeling frem for envejskommunikation**. Sidst, men ikke mindst, er det **uklart, hvad nytten af et øget samarbejde skal være**. Med andre ord er det en central udfordring at få afklaret samarbejdets fokus, formål og omfang med henblik på at etablere et interessefællesskab, som alle parter kan drage nytte af.

Indledning

Offentligt-privat samarbejde er på mange måder blevet *comme il faut* i moderne sikkerhedspolitik. Tidligere har sikkerhed været statens eksklusive ansvarsområde, men i takt med at trusselsbilledet er blevet mere diffust, omskifteligt og uforudsigeligt, ses det i stigende grad som nødvendigt at involvere den private sektor som (med)ansvarlig i arbejdet med at håndtere udfordringerne fra alt lige fra terrorisme til klimaforandringer. Denne tendens er tydelig i USA, hvor der alene i regi af Department for Homeland Security og FBI er etableret over 100 af sådanne sikkerhedspolitiske partnerskaber. I Danmark er omfanget ikke nær så stort, og vi har endnu ikke set den samme institutionalisering af partnerskaber på det sikkerhedspolitiske område. Der hersker dog ingen tvivl om, at virksomhedernes sikkerhed anses for at være relevant for nationens sikkerhed – også i Danmark. Direkte adspurgt svarer virksomheder i både Danmark[1] og udlandet da også, at de jævnligt er i kontakt med myndighederne vedrørende virksomhedernes sikkerhed.

Den store udbredelse af informations- og kommunika-

tionsteknologi (IKT) og trusler mod og gennem IKT bidrager i særlig grad til denne efterspørgsel efter sikkerhedspolitiske partnerskaber. Den stigende digitalisering betyder en stigende mangfoldighed og usikkerhed med hensyn til, hvem der påvirkes og dermed må tage konsekvenserne af disse trusler. Størstedelen af IKT-infrastrukturen er dog privatejet og –drevet og er derfor ikke underlagt den samme statslige myndighedskontrol, som sikkerhedspolitikken normalt foreskriver. Det særegne ved truslerne på dette område er desuden (jf. de nyeste *incident reports* fra Verizon og Mandiant), at der kan gå lang tid fra en IKT-relateret sikkerhedshændelse til, hændelsen opdages. Dette skaber et politisk behov for alternative muligheder for en robust og fleksibel håndtering af potentielle sikkerhedsmæssige problemstillinger.

Bekymringen for sikkerheden på dette område deles af virksomhederne. I gennemsnit er 93% af de adspurgte virksomheder fra bl.a. USA (98%), Storbritannien (90%) og Sverige (96%) "meget enige" eller "enige" i, at IT- og cybersikkerhed er en bekymring for virksomhedens sikkerhed. Denne tendens gør sig også gældende i en dansk kontekst (85%). I PwC's seneste *cybercrime* survey blandt danske virksomheder svarede 59 % af de deltagende virksomheder, at de har oplevet en hændelse, mens 68 % er mere bekymrede for cybertruslen nu end for 12 måneder siden. IKT-relaterede sikkerhedsspørgsmål er altså af betydning for såvel de offentlige myndigheder som den private sektor. Mens der er bred enighed om, at der er væsentlige udfordringer på dette område, er der forskelle i måden offentlige myndigheder og private virksomheder håndterer disse til tider overlappende sikkerhedsspørgsmål.

Baseret på en større interviewundersøgelse foretaget blandt offentlige og private aktører[2] samt en survey, som kortlægger relationen mellem private virksomheder og nationale efterretningstjenester i USA, UK, Sverige og Danmark[3], peger dette *policy brief* på tre væsentlige udfordringer og dilemmaer i forhold til at opnå et velfungerende samarbejde mellem de offentlige myndigheder og den private sektor om de sikkerhedsspørgsmål, som relaterer sig til IKT.

1. Andel af de adspurgte danske virksomheder, som er i kontakt med de følgende myndigheder mere end en gang om måneden: "Local police" 43,8%, "federal police and intelligence agencies" 18,8%, "emergency management services" 34,4%, "foreign service" 12,9%, "Department of Homeland Security or equivalent" 25% og "other" 20%.
2. Se side 11 for en liste over de interviewede.
3. 'Survey on Corporate Security Thinking', spørgeskema besvaret af 210 sikkerhedschefer i virksomheder i Storbritannien, USA, Sverige og Danmark. Gennemført af Karen Lund Petersen i 2011.

Trusselsbillede

Offentlige og private parter ser forskelligt på truslerne og organiserer sig ligeledes forskelligt.

Ikke overraskende er sikkerhedsspørgsmål relateret til IKT blevet genstand for stor politisk bevågenhed i de senere år; dette kommer bl.a. til udtryk i National strategi for cyber- og informationssikkerhed. IKT er integreret i alt – lige fra den enkelte borgers hverdag til en lang række samfundsvigtige funktioner. Kort sagt gennemsyrer IKT vores samfund. Det stiller vores samfund over for en række nye udfordringer. Den rivende teknologiske udvikling og brugernes stigende opfindsomhed betyder, at disse udfordringer er mangeartede og komplekse. De stammer ikke blot fra fjendtligsindede stater, men også fra ikke-statslige aktører med fjendtlige og/eller kriminelle hensigter, uforsigtige og uopmærksomme brugere, systemfejl, kompromitterede *mobile devices* etc. Disse mangfoldige og ofte diffuse trusler gør, at trusselsbilledet relateret til IKT er yderst komplekst og omskifteligt.

Adspurgt om den største forskel på IT-sikkerhed og andre sikkerhedstrusler svarer Chief Operational Risk Officer i Danmarks Nationalbank Thomas Baltzer Joensen:

"Forskellen i forhold til tidligere er et mere diffust og uforudsigeligt trusselsbillede. Angrebsfladen på IT-siden er hyperdynamisk og øges af nye teknologier, web-enablingen af systemer og data, graden af integration mellem parter, devices, netværk etc. samt forventningen om, at vores digitale identitet er tilgængelig 24/7/365 – uanset hvor på kloden vi befinder os."

En af konsekvenserne heraf er, at de offentlige myndigheder og de private virksomheder har forskellige forståelser af de udfordringer og trusler, som relaterer sig til IKT, samt deres håndtering. Disse forskelle kommer til udtryk i myndighedernes og virksomhedernes respektive tilgange og organisering på området. Blandt de offentlige myndigheder fordeles opgaverne primært mellem Center for Cybersikkerhed (CfCS), Politiets Efterretningstjeneste (PET) og Nationalt Cyber Crime Center (NC3) – og i mindre grad også Digitaliseringsstyrelsen og Statens IT (se figur 1). Denne opdeling beror i vid udstrækning på muligheden for at opretholde den klassiske distinktion mellem national sikkerhed (CfCS og PET) og kriminalitet (NC3) og tilstræber en kategorisering og fordeling af opgaverne derefter. Det er dog meningen, at CfCS skal være den samlende myndighed i sin funktion som national IT-sikkerhedsmyndighed, men centrets nuværende hovedfokus er mere snævert på APT-angreb og andre sofistikerede, eksterne trusler.[4] Centret udgiver dog også mere lavpraktiske rådgivende publikationer så som "It-sikkerhed på rejsen", hvilket mudrer billedet en smule. Ydermere anlægger myndighederne som udgangspunkt et nationalt perspektiv, i og med at fokus er på trusler rettet mod Danmark og danske samfundsvigtige funktioner.

I modsætning til de offentlige myndigheder anlægger virksomhederne i sagens natur et mere holistisk perspektiv på de IKT-relaterede trusler og udfordringer og skelner ikke på samme måde mellem de forskellige typer trusler og udfordringer. Virksomhederne er således mindre optagede af, om en hændelse er fx kriminalitet eller en potentiel trussel mod national sikkerhed, da hændelsen under alle omstændigheder har konsekvenser for virksomhedens drift eller rygte; de skadelige konsekvenser forbundet med hændelsen kan potentielt være lige problematiske for virksomhederne.

I virksomhederne er der således mindre fokus på trusselsaktørerne og mere på metoderne, sårbarhederne og konsekvenserne i forbindelse med en hændelse, da det er her, man kan sætte ind med forbedringer af virksom-

hedernes eget beredskab. Sårbarheder og trusler relateret til IKT er som sådan et vilkår, som langt hen ad vejen kan imødekommes ved at sikre systemer og arbejdsgange samt risikovurdere potentielle nye tiltag med udgangspunkt i den enkelte virksomheds risikoappetit. De virksomheder, der opererer globalt, ser derfor heller ikke kun på trusler mod deres danske netværk. For disse virksomheder er afgrænsningen af spørgsmålet om IKT-relateret sikkerhed til en dansk kontekst altså mindre relevant, og flere af virksomhederne sidder derfor også med i internationale samarbejdsfora på området.

Denne divergens mellem offentlige instanser og private virksomheder kommer også til udtryk i brugen af forskellige begreber på området. De forskellige aktører bruger forskellige begreber til at referere til IKT-relaterede sikkerhedsspørgsmål. Hvor man hos de offentlige myndigheder typisk taler om cybersikkerhed og cyberkriminalitet, taler de private virksomheder i højere grad om fx informationssikkerhed, IT-sikkerhed og datasikkerhed. Cybersikkerhed ses ofte – også blandt virksomhederne – som en delmængde, der refererer til CfCS' fokusområde: Beskyttelse af samfundsvigtig infrastruktur mod APT- og andre sofistikerede, eksterne angreb. Denne reference til samfundsvigtige funk-

FIGUR 1:

ANSVARSFORDELING MELLEM MYNDIGHEDER PÅ CYBER- OG INFORMATIONSSIKKERHEDSOMRÅDET

CfCS	PET	NC3	Digitaliseringsstyrelsen
National IT-sikkerheds-myndighed	National sikkerheds-myndighed	Politiets cyber crime center	Rådgivning af statslige myndigheder
• Fokus på særligt avancerede trusler fra udlandet mod kritisk infrastruktur	• Fokus på trusler mod nationens sikkerhed og fysisk sikring af information	• Fokus på forebyggelse, efterforskning og opklaring af IT-kriminalitet mod borgere og SMV'er	• Fokus på at statslige myndigheder lever op til obligatoriske principper
• Nationalt kompetencecenter på cybersikkerheds–området	• IT-sikkerheds-myndighed på Justitsministeriets område		• Publicerer materiale om informations-sikkerhed rettet mod borgere og statslige myndigheder

tioner og nationens sikkerhed er med til at opprioritere cybersikkerhedsspørgsmålet i forhold til andre udfordringer og trusler, om end det er almindelig anerkendt, at det kun udgør max. 5% af det samlede trusselsbillede. Til trods for sin koordinerende funktion repræsenterer CfCS altså kun et snævert udsnit af det trusselsbillede, virksomhederne oplever i deres dagligdag.

De divergerende trusselsbilleder medfører således en række udfordringer for samarbejdet mellem myndigheder og virksomheder. Overordnet set er det naturligvis en udfordring for et velfungerende samarbejde, når der er uenighed om trusselsbilledet og prioriteringen af de forskellige udfordringer i forhold til hinanden. Disse forskelle gør det også svært for virksomhederne at vide, hvor de skal henvende sig hos de offentlige myndigheder, når statens inddeling af truslerne ikke stemmer overens med deres eget trusselsbillede. Formand for Rådet for Digital Sikkerhed, Rasmus Theede, udtrykker problemet således:

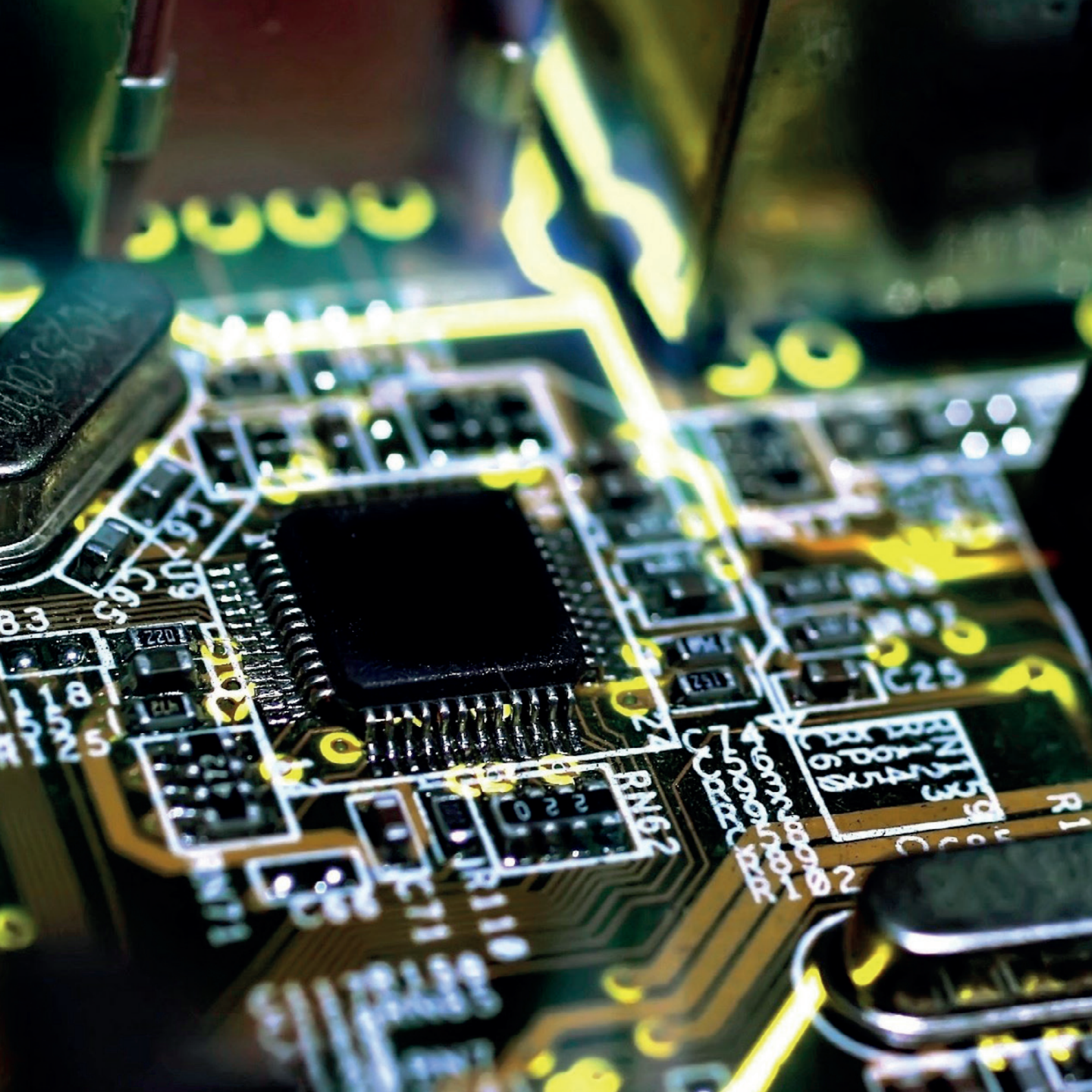
"Som borger og virksomhed er det ofte svært at finde ud af, hvor man skal henvende sig, og hvem der har ansvaret. Folk må ofte gå forgæves på deres lokale politistation, og det er for mange svært at kende forskellen på de mange aktører som NC3, Center for Cybersikkerhed, private aktører med mere."

De forskellige opfattelser af trusselsbilledet besværliggør også ansvarsfordelingen mellem myndigheder og virksomheder. Sidstnævnte står først og fremmest til ansvar over for deres aktionærer, om end virksomheder med ansvar for kritisk infrastruktur er underlagt specifikke regler og forpligtelser; men de har stadig fokus på at skabe størst mulig værdi. Virksomhederne skal dog stadig – selvom de ikke selv arbejder med denne inddeling – vurdere, hvornår en given hændelse skal kategoriseres som et myndighedsanliggende – og hvilken myndighed der i så fald skal rettes henvendelse til.

Samlet kan udfordringerne relateret til trusselsbilledet opsummeres således:

- Virksomheder og myndigheder har forskellig forståelse af, hvad den primære trussel er, og hvordan den skal behandles. Virksomhederne er optaget af alle potentielle trusler mod deres kerneprodukter og aktiviteter, mens myndighederne har institutionaliseret en opdeling af IKT-relaterede trusler i relation til det trusselsniveau, de udgør mod samfundet.
- Virksomheder fokuserer mere på metoderne, sårbarhederne og konsekvenserne i forbindelse med en hændelse og i mindre grad på aktøren.
- Det er uklart, hvilke myndigheder virksomhederne skal henvende sig til for at få hjælp, da både truslens karakter og potentielle samfundsmæssige værdi ofte er uklar eller ukendt.
- Modsat danske myndigheder skelner store virksomheder ikke mellem nationale og internationale IKT-hændelser.

4. Center for Cybersikkerheds fokus på eksterne trusler følger også af National strategi for cyber- og informationssikkerheds skelnen mellem henholdsvis cyber- og informationssikkerhed. Hvor sidstnævnte er "…en bred betegnelse for de samlede foranstaltninger til at sikre informationer i forhold til fortrolighed, integritet (ændring af data) og tilgængelighed", defineres cybersikkerhed som "beskyttelse imod de sikkerhedsbrud, der opstår som følge af angreb mod data eller systemer via en forbindelse til et eksternt net eller system".


C25
RN62

Kommunikationsformer **Der efterspørges mere dialog frem for envejskommunikation.**

I forhold til sikkerhedspolitiske spørgsmål har der historisk været skelnet skarpt mellem staten og den private sektor. Sikkerhedspolitikken var statens prærogativ. I takt med at trusselsbilledet er blevet mere diffust og uforudsigeligt, er den traditionelle arbejdsfordeling dog blevet udfordret; skellet mellem staten og den private sektor er blevet mere flydende og er i stigende grad til forhandling. Grundet den store udbredelse af IKT, og i og med at størstedelen af den samfundsvigtige IKT-infrastruktur ejes og drives af private virksomheder, fordrer håndtering af IKT-relaterede sikkerhedsspørgsmål også involvering af virksomhederne. Spørgsmålet er nu, i hvilket omfang virksomhederne skal gøres til medansvarlige for nationens sikkerhed, og i hvilket omfang staten skal tage ansvar for virksomhedernes sikkerhedsmæssige udfordringer. Afhængig af svaret på dette spørgsmål er der behov for at evaluere forskellige former for kommunikation.

I den nuværende inddragelse af private virksomheder i arbejdet med IKT-relaterede sikkerhedsspørgsmål har kortlægningen vist, at der primært er tale om envejskommunikation. Kommunikationen foregår primært gennem møder, hvor myndighederne indkalder virksomhederne og informerer dem om trusler og tendenser. De offentlige myndigheder styrer således i udpræget grad, hvilke informationer de ønsker at dele med virksomhederne – og hvilke de ønsker at hemmeligholde. Dermed ligger prioriteringen af de forskellige udfordringer og truslers relevans for offentlig-privat samarbejde også hos myndighederne. Denne kommunikationsform lægger sig tæt op ad den traditionelle tilgang til sikkerhedspolitik, da det stadig er staten, som styrer. Således beskriver Thomas Lund-Sørensen, chef for CfCS, også det nuværende samarbejde:

" Det [CfCS' interessentforum] er et forum, hvor 75 % af kommunikationen er fra os til dem og 25 % den anden vej, og der ville vi gerne have en bedre balance."

Fra flere sider efterspørges en anden kommunikationsform – en som i højere grad baserer sig på tillid, dialog og konsensus. Der efterspørges en kommunikationsform, hvor man i fortrolighed kan dele og diskutere sine erfaringer, bekymringer og behov. Dertil efterspørger flere af virksomhederne en langt mere operativ, dag-til-dag tilgang med kortere reaktionstid på nye trusler. Chief Information Security Officer i DONG Martin Warming påpeger således behovet for dialog med henvisning til det omskiftelige trusselsbillede:

"Hvis der skal være et samarbejde, der virker, skal det være mere operationelt og hurtigt. Der skal være næsten daglig kontakt, eller noget der er meget mere ping-pong frem og tilbage, hvis det skal virke – netop fordi det er et arms-race."

Dermed lægges der op til et samarbejde baseret på fælles prioritering og håndtering af de relevante trusler og udfordringer. Med andre ord efterspørges det, at virksomhederne i højere grad skal inddrages som ligeværdige partnere, frem for at styringen centraliseres hos de offentlige myndigheder.

Kommunikationsformen er altså i høj grad med til at præge samarbejdet og ikke mindst selve sikkerhedspolitikken på området. Der er tale om vidt forskellige former for ansvarsfordeling og vidensproduktion. Derfor er det en væsentlig udfordring at få afklaret, hvilken form for samarbejde, man ønsker, og hvilken kommunikationsform der skal til for at understøtte den.

Samlet set er udfordringen:

- At skabe en ramme for samarbejde, som i højere grad baseres på dialog, men som samtidig ikke kompromitterer statens ansvar for håndtering af trusler mod nationen.

Nytte **Det er uklart, hvad nytten af samarbejdet skal være.**

Et væsentligt spørgsmål i forhold til kommunikationsformen er desuden, hvad der skal kommunikeres om. Der er som nævnt en generel efterspørgsel efter øget dialog og vidensdeling blandt såvel offentlige som private aktører. Ikke desto mindre er det uklart, hvad der mere konkret skal komme ud af dette. Der peges på, at det nuværende samarbejde primært foregår på et strategisk niveau, hvor man diskuterer generelle trends, men at dette ikke i sig selv er brugbart i forhold til konkrete trusler og hændelser; virksomhederne er i vid udstrækning allerede bekendte med de konkrete trusler og hændelser, som fremhæves på de nuværende møder. Derfor efterspørger flere virksomheder et mere operativt samarbejde i stedet for eller som supplement til det strategiske, hvor man løbende kan udveksle viden om specifikke hændelser og rådgive hinanden om håndteringen af disse.

De fleste virksomheder, som har deltaget i interviewundersøgelsen, er i private netværk med andre private virksomheder, hvor man allerede udveksler viden på såvel det strategiske som det operative niveau. De potentielle deltagere i et offentlig-privat samarbejde på området har dog ikke uendelige ressourcer til at deltage i forskellige fora og netværk. Derfor skal et offentlig-privat samarbejde kunne bidrage med merværdi i forhold til de eksisterende fora og netværk, men det er uklart, hvad særligt virksomhederne kan få ud af et samarbejde, som de ikke allerede får ud af deres private netværk.

I denne henseende er det vigtigt, hvad henholdsvis myndighederne og virksomhederne rent faktisk kan og vil bidrage med til samarbejdet. Som nævnt ovenfor er det i det nuværende samarbejde primært myndighederne, der styrer informationsflowet. Spørgsmålet er derfor, i hvilket omfang myndighederne ønsker at slække på denne styring og dele ansvaret med virksomhederne – samt med hvilket formål. Myndighederne skal altså tage stilling til, hvilken konkret nytteværdi de ønsker at få ud af et eventuelt samarbejde og afveje det mod at dele mere med virksomhederne.

Spørgsmålet er ligeledes, hvor meget ansvar virksomhederne ønsker at tage. Til trods for deres ønske om i højere grad at blive inddraget, fremhæver de tydeligt, at de ikke ønsker at blive stillet ansvar for Danmarks nationale sikkerhed på området som en del af et offentlig-privat samarbejde og dermed potentielt ende i en offentlig gabestok i medierne. Spørgsmålet er desuden, hvor mange ressourcer virksomhederne er parate til at allokere til et samarbejde i forhold til at få en egentlig merværdi ud af samarbejdet. Ud over et lettere diffust ønske om øget vidensdeling fra både offentlige og private aktører fremstår det altså uklart, hvad de enkelte deltagere kan og vil bidrage med til et samarbejde. Kim Aarenstrup, chef for NC3, er dog opmærksom på, at et eventuelt samarbejde også skal have værdi for virksomhederne:

"Jeg tror, den største hindring for at komme derhen er, at vi ikke formår at skabe værdi for virksomhederne i det her samarbejde. Det er rigtig vigtigt, at vi har værdiskabelse fra dag ét, for de er jo konkurrencesøgende virksomheder ude

i markedet […] Vi skal vide, hvordan vi leverer noget af en tilsvarende kvalitet den anden vej. Det er dét, som det hele står og falder med. […] Man skal være opmærksom på, at for at få et public-private partnership er man nødt til at arbejde med værdiskabelse."

Sidst, men ikke mindst, er det nødvendigt at få afklaret, hvad man ønsker at samarbejde – og dermed vidensdele – om. Som følge af den ovennævnte uoverensstemmelse mellem myndighedernes og virksomhedernes trusselsbilleder består en væsentlig udfordring i at blive enige om, hvorvidt man skal begrænse samarbejdet til "cybersikkerhed", eller man skal samarbejde om det brede trusselsbillede. Ydermere er der også spørgsmålet om, hvorvidt samarbejdet skal begrænse sig til trusler, der retter sig specifikt mod danske mål, eller om man også skal inkludere internationale netværk, som er relevante for flere af virksomhederne. I logisk forlængelse af disse afklaringer følger spørgsmålet om, hvilke virksomheder der er relevante i forhold til samarbejdet. Er det en bestemt type virksomheder – kræver det en vis størrelse, en bestemt type udfordringer, et vist modenhedsniveau, at man er en del af samfundsvigtige funktioner etc. – eller er samarbejdet potentielt set åbent for alle?

Samlet set er udfordringen:

- At afklare samarbejdets fokus, formål og omfang.
- Virksomhederne efterspørger operativt samarbejde og ikke blot strategisk informationsudveksling.
- Nye privat-offentlige partnerskaber skal supplere brugen af private netværk og derved bidrage med merværdi.
- Virksomhederne ønsker ikke at blive holdt ansvarlige for den nationale sikkerhed.
- At etablere et interessefællesskab, som alle parter kan drage nytte af.

Konklusion

- Offentlige og private aktører har forskellige opfattelser af trusselsbilledet relateret til IKT. Dette er en udfordring for partnerskaber og samarbejde, da der dermed ikke er enighed om, hvad der skal samarbejdes om.
- Den nuværende kommunikation mellem offentlige og private aktører er kendetegnet ved at være kontrolleret af statslige aktører og foregå på strategisk niveau. Dette udfordrer de operative behov, private aktører har, ligesom det besværliggør dialog og formulering af en fælles forståelse af truslerne.
- Det er uklart, hvad værdien og nytten af eventuelle partnerskaber skal være for de respektive aktører. Virksomheder har som hovedformål at skabe værdi, hvilket dermed også bliver et krav til sådanne partnerskaber. Myndigheder kan dermed blive tvunget til at opbløde deres egen forståelse af sikkerhed og kriminalitet. Dette kan udfordre de demokratiske samfunds traditionelle forståelse af forholdet mellem normal- og sikkerhedspolitik og kræver derfor også grundige politiske overvejelser.

December 2015

Ph.d.-stipendiat Kristoffer Kjærgaard Christensen (kk@ifs.ku.dk)
Videnskabelig assistent Oscar Vejen Lacoppidan
Lektor Karen Lund Petersen (klp@ifs.ku.dk)

CAST og NordSTEVA

Interviews

- Carlsberg, Klaus Høj Tipsmark
- Center for Cybersikkerhed, Thomas Lund-Sørensen
- CERTA Intelligence and Security, Morten Kähler
- Dansk Industri, Henning Mortensen
- Danske Bank, Poul Otto Schousboe
- Digitaliseringsstyrelsen, Cecilie Christensen
- DONG, Martin Warming
- Energistyrelsen, Jens Christian Vedersøe
- FBI, Charles Esposito
- Microsoft, Ole Kjeldsen
- Mærsk, Bent Larsen
- Nationalbanken, Thomas Baltzer Joensen
- NC3, Kim Aarenstrup
- PET, Jesper Laisen
- Rådet for Digital Sikkerhed, Rasmus Theede
- Statens IT, Vibe Vallentin Jensen
- Systematic, Rune Raunow
- TDC, Lars Højberg og Kurt Sejr Hansen
- TRYG Forsikring, Tom Engly
- Udenrigsministeriet, Jesper Ullerup

LAYOUT: SIGNS & WONDERS